(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. April 2004 (01.04.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/028076 A1

(51) Internationale Patentklassifikation[7]: H04L 9/32

(21) Internationales Aktenzeichen: PCT/EP2003/010327

(22) Internationales Anmeldedatum:
17. September 2003 (17.09.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
02020818.7 17. September 2002 (17.09.2002) EP

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder; und

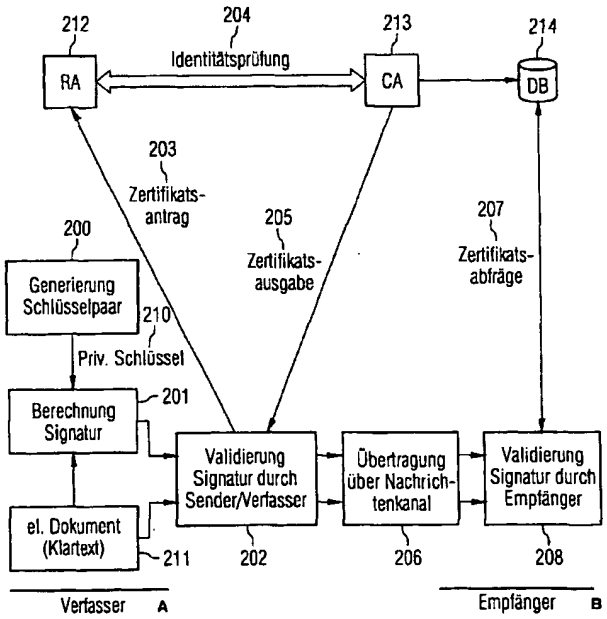
(75) Erfinder/Anmelder *(nur für US)*: **HEINTEL, Markus** [DE/DE]; Josef-Retzer-Str. 29, 81241 München (DE). **FURCH, Andreas** [DE/DE]; Moosstrasse 88, 85356 Freising (DE). **FRANKE, Markus** [DE/DE]; Gute Änger 26, 85356 Freising (DE). **PFAFF, Oliver** [DE/DE]; Grossgörschenstr. 5, 10827 Berlin (DE).

(74) Gemeinsamer Vertreter: **SIEMENS AKTIENGESELLSCHAFT**; Postfach 22 16 34, 80506 München (DE).

*[Fortsetzung auf der nächsten Seite]*

(54) Title: METHOD FOR GENERATING AND/OR VALIDATING ELECTRONIC SIGNATURES

(54) Bezeichnung: VERFAHREN ZUR ERZEUGUNG UND/ODER VALIDIERUNG ELEKTRONISCHER SIGNATUREN




200 GENERATION OF KEY PAIR
201 CALCULATION OF SIGNATURE
202 VALIDATION OF SIGNATURE BY SENDER/AUTHOR
203 CERTIFICATE REQUEST
204 VERIFICATION OF IDENTITY
205 ISSUE OF CERTIFICATE
206 TRANSMISSION VIA MESSAGE CHANNEL
207 CERTIFICATE INQUIRY
208 VALIDATION OF SIGNATURE BY RECIPIENT
210 PRIVATE KEY
211 ELECTRONIC DOCUMENT (PLAINTEXT)
A AUTHOR
B RECIPIENT

(57) **Abstract:** The invention relates to a method for generating and/or validating electronic signatures during which an asymmetric key pair is generated that comprises a private signature key and a public validation key. In addition, at least one electronic signature is calculated by using the private signature key and by applying a predeterminable signature function for at least one electronic document. A certification of the public validation key ensues after the calculation of the at least one electronic signature.

(57) **Zusammenfassung:** Die Erfindung betrifft ein Verfahren zur Erzeugung und/oder Validierung elektronischer Signaturen, bei dem ein asymmetrisches Schlüsselpaar erzeugt wird, das einen privaten Signaturschlüssel und einen öffentlichen Validierungsschlüssel umfasst. Ausserdem wird zumindest eine elektronische Signatur mittels des privaten Signaturschlüssels und durch Anwendung einer vorgebbaren Signaturfunktion für zumindest ein elektronisches Dokument berechnet. Nach

*[Fortsetzung auf der nächsten Seite]*

WO 2004/028076 A1